**Yee & Associates, P.C.**

4100 Alpha Road
Suite 1100
Dallas, Texas 75244

Main No. (972) 385-8777
Facsimile (972) 385-7766

RECEIVED
CENTRAL FAX CENTER

AUG 16 2005

# Facsimile Cover Sheet

| | |
|---|---|
| To: Commissioner for Patents for<br>**Examiner Longbit Chai**<br>**Group Art Unit 2131** | Facsimile No.: **571/273-8300** |
| From: Lourdes Perez<br>Legal Assistant to Wing Yan Mok | No. of Pages Including Cover Sheet: **25** |
| Message:<br><br>Enclosed herewith:<br><br>• Transmittal Document; and<br>• Appeal Brief. | |
| Re: Docket No: **AUS920010242US1** | Serial No. **09/931,301** |
| Date: Tuesday, August 16, 2005 | |
| **Please contact us at (972) 385-8777 if you do not receive all pages indicated above or experience any difficulty in receiving this facsimile.** | *This Facsimile is intended only for the use of the addressee and, if the addressee is a client or their agent, contains privileged and confidential information. If you are not the intended recipient of this facsimile, you have received this facsimile inadvertently and in error. Any review, dissemination, distribution, or copying is strictly prohibited. If you received this facsimile in error, please notify us by telephone and return the facsimile to us immediately.* |

PLEASE CONFIRM RECEIPT OF THIS TRANSMISSION BY FAXING A CONFIRMATION TO 972-385-7766.

**IN THE UNITED STATES PATENT AND TRADEMARK OFFICE**

In re application of: **Black et al.**

Serial No.: **09/931,301**

Filed: **August 16, 2001**

For: **Presentation of Correlated Events as Situation Classes**

§ Group Art Unit: **2131**

§

§ Examiner: **Chai, Longbit**

§

§ Attorney Docket No.: **AUS920010242US1**

§



**Certificate of Transmission Under 37 C.F.R. § 1.8(a)**
I hereby certify this correspondence is being transmitted via facsimile to the Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450, facsimile number (571) 273-8300 on August 16, 2005.

By: Lourdes Perez

35525
PATENT TRADEMARK OFFICE
CUSTOMER NUMBER

## TRANSMITTAL DOCUMENT

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:
ENCLOSED HEREWITH:

- Appeal Brief (37 C.F.R. 41.37)

A fee of $500.00 is required for filing an Appeal Brief. Please charge this fee to IBM Corporation Deposit Account No. 09-0447. No additional fees are believed to be necessary. If, however, any additional fees are required, I authorize the Commissioner to charge these fees which may be required to IBM Corporation Deposit Account No. 09-0447. No extension of time is believed to be necessary. If, however, an extension of time is required, the extension is requested, and I authorize the Commissioner to charge any fees for this extension to IBM Corporation Deposit Account No. 09-0447.

Respectfully submitted,

Wing Yan Mok
*Registration No. 56,237*
AGENT FOR APPLICANTS

Duke W. Yee
*Registration No. 34,285*
ATTORNEY FOR APPLICANTS

YEE & ASSOCIATES, P.C.
P.O. Box 802333
Dallas, Texas 75380
(972) 385-8777

08/17/2005 TL0111 00000041 090447 09931301
01 FC:1402 500.00 DA

**Docket No. AUS920010242US1**

***PATENT***



**IN THE UNITED STATES PATENT AND TRADEMARK OFFICE**

| | | |
|---|---|---|
| In re application of: **Black et al.** | § | |
| | § | Group Art Unit: **2131** |
| Serial No. **09/931,301** | § | |
| | § | Examiner: **Chai, Longbit** |
| Filed: **August 16, 2001** | § | |
| | § | |
| For: **Presentation of Correlated Events as Situation Classes** | § | |

**Commissioner for Patents**
**P.O. Box 1450**
**Alexandria, VA 22313-1450**

**Certificate of Transmission Under 37 C.F.R. § 1.8(a)**
I hereby certify this correspondence is being transmitted via facsimile to the Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450, facsimile number (571) 273-8300 on August 16, 2005.

By: Lourdes Perez
Lourdes Perez

## APPEAL BRIEF (37 C.F.R. 41.37)

This brief is in furtherance of the Notice of Appeal, filed in this case on July 21, 2005.

The fees required under § 41.20(B)(2), and any required petition for extension of time for filing this brief and fees therefore, are dealt with in the accompanying TRANSMITTAL OF APPEAL BRIEF.

## REAL PARTY IN INTEREST

The real party in interest in this appeal is the following party: International Business Machines Corporation.

## RELATED APPEALS AND INTERFERENCES

With respect to other appeals or interferences that will directly affect, or be directly affected by, or have a bearing on the Board's decision in the pending appeal, there are no such appeals or interferences.

## STATUS OF CLAIMS

### A. TOTAL NUMBER OF CLAIMS IN APPLICATION

Claims in the application are: 1-21

### B. STATUS OF ALL THE CLAIMS IN APPLICATION

1. Claims canceled: NONE
2. Claims withdrawn from consideration but not canceled: NONE
3. Claims pending: 1-21
4. Claims allowed: NONE
5. Claims rejected: 1-21
6. Claims objected to: NONE

### C. CLAIMS ON APPEAL

The claims on appeal are: 1-21

## STATUS OF AMENDMENTS

There are no amendments after final rejection.

## SUMMARY OF CLAIMED SUBJECT MATTER

### A. CLAIMS 1, 8 and 15 - INDEPENDENT

Independent claims 1, 8, and 15 of the present invention are directed to a method, a computer program product, and a data processing system for reporting security situations, comprising the steps of logging events by storing event attributes as an event set, wherein each event set includes a source attribute, a target attribute and an event category attribute; classifying events as groups by aggregating events with at least one attribute within the event set as an identical value; calculating severity levels for the groups; and reporting a group from the groups to a user as a situation, if a severity level of the group exceeds a threshold value. (Specification page 16, lines 15-28, Figure 9).

## GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

### A. GROUND OF REJECTION 1 (Claims 1-21)

Claims 1-21 stand rejected under 35 U.S.C. § 102(e) as allegedly anticipated by Molini (U.S. Patent No. 6,353,385 B1).

## ARGUMENT

### A. GROUND OF REJECTION 1 (Claims 1-21)

### A.1. 35 U.S.C. § 102(e), Alleged Anticipation, Claims 1-21

The Final Office Action rejects claims 1-21 under 35 U.S.C. § 102(e) as being allegedly anticipated by Molini (U.S. Patent No. 6,353,385 B1). This rejection is respectfully traversed.

As to claims 1, 8, and 15, the Final Office Action states:

> As per claim 1, 8, and 15, Applicants argues: "Molini does not teach classifying events as groups by aggregating events with at least one attribute within the event set as an identical value".
>
> Examiner notes, first of all, the event is interpreted as an undesired behavior pattern observed from a series of alarm messages with the following event attributes: source of attack, destination of attack and type of event or intrusion (or attack) (Molini: see for example, Column 5 Line 4-7). Secondly, Molini teaches classified the event groups with the appropriate severity level / priority level based on the determination whether the minimum threshold has been exceeded or not after aggregation those events with at lease one attribute with an identical value within the event set (Molini: see for example, Column 7 Line 5-6, Column 7 Line 35-37, Column 7 Line 50-55, Column 7 Line 60-61 and Column 5 Line 4-7). Examiner interprets "the attribute with an identical value within the event set" as, for example, unauthorized access type and particular computers (i.e. the same network address) to meet the claim language (Molini: see for example, Column 7 Line 60-61).
>
> Therefore, Molini does teach classifying events as groups by aggregating events with at lest one attribute within the event set as an identical value.

Final Office Action dated April, 21, 2005, pages 2-3.

A prior art reference anticipates the claimed invention under 35 U.S.C. § 102(e) only if every element of a claimed invention is identically shown in that single reference, arranged as they are in the claims. *In re bond*, 910 F .2d 831, 832, 15 U.S.P.Q.2d 1566, 1567 (Fed Cir. 1990). All limitations of the claimed invention must be considered when determining patentability. *In re Lowry*, 32 F.3d 1579, 1582, 21 U.S.P.Q.2d 1031, 1034 (Fed Cir. 1994). Anticipation focuses on whether a claim reads on the product or process a prior art reference discloses, not on what the reference broadly teaches. *Kalman v. Kimberly-Clark Corp.*, 713 F.2d 760, 218 U.S.P.Q. 781 (Fed. Cir. 1983). Appellants respectfully submit that Molini does not teach every element of the

claimed invention arranged as they are in claims 1, 8 and 15.

Independent claim 1, which is representative of claims 8 and 15 with regard to similarly recited subject matter, reads as follows:

> 1. A method in a data processing system for reporting security situations, comprising the steps of:
>
> logging events by storing event attributes as an event set, wherein each event set includes a source attribute, a target attribute and an event category attribute;
>
> classifying events as groups by aggregating events with at least one attribute within the event set as an identical value; and
>
> calculating severity levels for the groups;
>
> reporting a group from the groups to a user as a situation, if a severity level of the group exceeds a threshold value. (Emphasis added).

Molini does not teach the features emphasized above. As discussed in the Abstract, Molini teaches an alarm interface system that receives intrusion alarm messages from an intrusion detection system. The alarm interface system organizes a group of the intrusion alarm messages into a time sequence. A highest priority alarm message is selected from the group. An analyzer analyzes the highest priority alarm message to extract raw locale information. The raw locale information is translated into refined locale information (e.g. a zone identifier) for inclusion in a central station-compatible data message.

Instead of calculating a severity level for a group of events, Molini assigns a criticality level to each individual message. In the Final Office Action, the Examiner alleges that Molini teaches calculating severity levels for the groups at column 7, line 54 and line 33, where Molini teaches assigning a criticality level to the incoming alarm message according to criteria specified by a network operator of the target system and assigning a lower priority to an incoming message that indicates detection of probing in protected computer. The Examiner interprets the severity level calculated for each group as the criticality level or priority assigned to the incoming alarm message by Molini. The Examiner's allegation is incorrect.

Nowhere in the reference does Molini mention assigning a criticality level to a group of messages as a whole. In the presently claimed invention, events are classified as groups such that a severity level may be calculated and compared to a threshold. If the severity level of a group is above the threshold, the group is reported to the user. Molini does not teach such features. Instead of grouping the messages, Molini filters the incoming messages one message at a time and throws

away the message based on characteristics such as time of receipt (column 7, lines 1-5). Therefore, Molini does not teach calculating severity level for the groups as recited in claims 1, 8, and 15 of the present invention.

Instead of reporting to a user a group of event, Molini only assign a criticality level to an individual message. Since Molini does not teach calculating a severity level for a group of events, Molini would not teach reporting a group of events to the user if the severity level of the group exceeds the threshold value. In addition, nowhere in the reference does Molini even mention reporting messages to the user as a group. Therefore, Molini does not teach reporting a group of events to a user if the severity level of the group exceeds the threshold value.

Furthermore, instead of grouping messages based on the messages having an identical attribute value, Molini group messages based on a time of receipt of the messages. The Examiner alleges that Molini teaches classifying events as groups by aggregating events with at least one attribute within the event set as an identical value at column 7, lines 5-6, 27-40, 50-61 and at column 5, lines 4-7, which read as follows:

> The priority module **36** may assign a priority level to an incoming alarm message based on a characteristic of the incoming alarm message, such as time of receipt of the incoming alarm message at the receiver **32**, identity of the incoming alarm message, type of the incoming alarm message, or the like.

Column 7, lines 5-6.

> The priority module **36** may estimate a danger level of an attack based on the network address targeted by the attack, the judgment of the network operators, and historic occurrences of attacks and their disposition. Where possible, a priority module **36** identifies the network address of the targeted system that was targeted by the attack. The priority module **36** determines or assigns a criticality level to the incoming alarm message according to criteria specified by a network operator of the targeted system. The criticality levels indicate a significance to a network operator concerning an attack upon a corresponding network address. To this end, the priority module **36** may contain a database **15** for storage and retrieval of criticality levels associated with corresponding network addresses.

Column 7, lines 27-40.

> If the likelihood of success meets or exceeds a minimum threshold (e.g., greater than or equal to 10 percent), the priority module **36** may estimate the financial impact or severity of a successful attack on the victim (e.g., business entity) of the attack. For example, the priority module **36** may assign a lower priority to an incoming data message that indicates the detection of probing of the ports of the protected computer **16**, whereas the priority module **36** may assign a higher priority

> for an incoming data message that indicates an unauthorized user's illicit access of records of the internal computer **52** or the protected computer **16** because of the financial severity attendant with the illicit access.
>
> Column 7, lines 50-61.

> The intrusion alarm message **54** may include one or more of the following items: location or attributed source of the attack, destination of the attack, time stamp for when the attack occurred, type of the even or intrusion, descriptive information, and alarm flags.
>
> Column 5, lines 4-7.

In these sections, Molini merely teaches a priority module that assigns a priority level to an incoming message based on a characteristic of the incoming message, for example, a time of receipt, an identity of the message, a type of the message, etc. In addition, Molini teaches that the priority module determines or assigns a criticality level to the message according to criteria specified by network operator, which indicates a significance to a network operator concerning an attack upon a network address targeted by an attack. The priority module assigns a higher priority to an incoming message that indicates an unauthorized access of records of an internal or personal computer.

However, the priority module that Molini teaches does not classify incoming messages as groups by aggregating messages that have at least one attribute within an event set as an identical value. The Examiner states in the Response to Arguments section of the Final Office Action that he interprets the "at least one attribute within the event set" as recited in the claim as the unauthorized access type and particular computers that have the same network address in Molini. The Examiner's allegation is erroneous. Molini does not classify incoming messages as groups based on either an identical unauthorized access type or an identical network address. Molini merely teaches that the priority module assigns a message with a high criticality level if the network operator's concern of an attack upon a network address is significant. Similarly, Molini teaches that the priority module assigns a higher priority to a message if the message indicates an unauthorized access. Assigning a criticality level that indicates significance to the network operator and assigning a higher priority to messages that indicate unauthorized access are not the same as classifying messages as groups by aggregating messages that have at least one attribute as an identical value. Molini assigns a criticality level or a higher priority to incoming messages in order to rank the messages such that the highest priority message may be output to the analyzer

(column 6, lines 65-67 and column 8, lines 13-14). Assigning to incoming messages a criticality level indicating a significance or a higher priority indicating unauthorized access do not classify the messages as groups in any way, let alone classifying messages as groups based on the aggregating messages that have an identical attribute value. Assigning a criticality level or a higher priority to incoming messages merely helps Molini in ranking the messages. Therefore, the Examiner's allegation is erroneous.

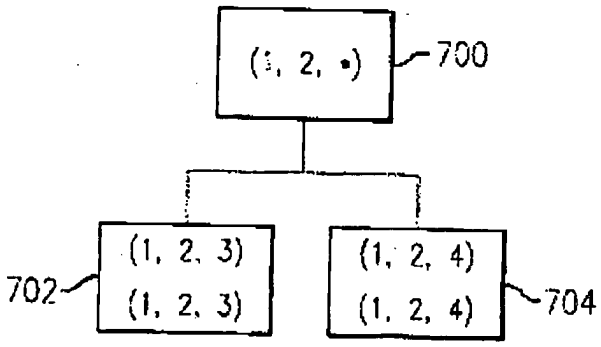
In addition, contrary to the presently claimed invention, Molini teaches away from classifying messages as groups with at least one event attribute within an event set as an identical value by specifically organizing incoming messages into a sequential group based on a time sequence at column 6, lines 52-63, which reads as follows:

> The sequencer **34** evaluates the incoming data messages within a window of time to define a sequential group of data message. Similarly, the priority module **36** evaluates the priority within each sequential group. The window may be determined based on the time of receipt of the incoming data messages arrive at the receiver **32**. In one embodiment, the console operator may specify a window of varying duration on a per-system basis. The time window prevents the alarm interface system **30** from waiting for an indeterminate time, expecting a new message to appear from the intrusion detection system **28**. In practice, the alarm interface system **30** operates on a series of successive windows.

Column 6, lines 52-63.

In the above section, Molini teaches that incoming messages are grouped based on a window of time, which may be determined based on the time of receipt of the messages. Thus, Molini's teaching is different from the presently claimed invention in that Molini classifies messages as groups based on the time of receipt of the messages instead of aggregating messages that have an identical attribute value. As described in **Figure 7**, which is illustrated below, and on page 14, lines 7-18 of the current specification, events are grouped by aggregating events that have at least one event attribute within an event set as an identical value. For example, group **700** is a group of events that have a source attribute of **1** and a target attribute of **2**. Group **702** is a group of events that have an event category of **3**, and group **704** is a group of events that have an event category of **4**.

FIG. 7




Molini does not teach such features. To the contrary, Molini teaches grouping incoming messages sequentially based on a time of receipt of the messages. Therefore, Molini does not teach the features as recited in claims 1, 8, and 15 of the present invention.

Furthermore, Molini could not have classified messages as groups based on an identical network address or an identical unauthorized access type as alleged by the Examiner. At column 6, line 64 to column 7, line 5, Molini teaches that the priority module determines the highest priority message within the sequential group in accordance with a priority scheme and then assigns a priority level to the message based on the a characteristic of the message. In other words, the priority module does not assign a priority to messages until after the sequential group is formed based on the time of receipt of the messages. Thus, Molini could not have classified messages as groups based on the unauthorized access type or a corresponding network address, since the messages have to be sequentially grouped first before the priority module can assign the priority. Therefore, Molini could not teach classifying messages as groups with at least one event attribute within an event set as an identical value, as recited in claims 1, 8, and 15 of the present invention.

Thus, instead of calculating a severity level for each group of events, Molini only teaches assigning criticality level to an individual message. Instead of grouping messages based on the messages having an identical attribute value, Molini group messages based on the time of receipt of messages. Instead of report the messages to a user as a group, Molini only assigns the criticality level to one message at a time. Looking at the features as a whole, Appellants respectfully submit that Molini does not teach the features of claims 1, 8 and 15. At least by virtue of their dependency on claims 1, 8 and 15 respectively, Molini does not teach or suggest

the features of dependent claims 2-7, 9-14, and 16-21. Accordingly, Appellants respectfully request the withdrawal of the rejection of claims 1-21 under 35 U.S.C. § 102(e).

In addition, Molini does not teach the specific features of claims 2-7, 9-14, and 16-21 of the present invention. For example, with regard to dependent claim 2, which is representative of dependent claims 9 and 16 with regard to similarly recited subject matter, instead of calculating severity levels for the groups based on at least one of the number of event sets within each of the groups, the source attribute of the event sets within each of the groups, the target attribute of the event sets within each of the groups, and the event category attribute of the event sets within each of the groups, Molini only assigns a criticality level to an individual message..

The Examiner alleges that Molini teaches these features at column 7, lines 5-6, 35-37, lines 50-55, 60-61, column 5, lines 4-7, which are reproduced above, and at column 7, lines 27-40 and column 8, lines 48-55, which read as follows:

> The priority module **36** may estimate a danger level of an attack based on the network address targeted by the attack, the judgment of the network operators, and historic occurrences of attacks and their disposition. Where possible, a priority module **36** identifies the network address of the targeted system that was targeted by the attack. The priority module **36** determines or assigns a criticality level to the incoming alarm message according to criteria specified by a network operator of the targeted system. The criticality levels indicate a significance to a network operator concerning an attack upon a corresponding network address. To this end, the priority module **36** may contain a database **15** for storage and retrieval of criticality levels associated with corresponding network addresses.

Column 7, lines 27-40.

> The probability of having a valid locale for the attack may be higher if the local is based upon the both the extraction of the destination indictor and the source indicator of the attack from the highest priority intrusion alarm message **54**. Conversely, the probability for having a valid locale for the attack may be lower if based solely on the extracted destination indicator or the extracted source indicator. The analyzer **38** communicates with a translator **40**.

Column 8, lines 48-55.

In these sections, Molini teaches that the priority module assigns a criticality level to the incoming message, which indicates a significance to network operator concerning an attack upon a corresponding network address. Molini also teaches an analyzer that can extract destination address and source address of the attacking message in order to assign a probability indicator that indicates a probability of having a valid locale for an attack. However, nowhere in the above sections, or

any other section, in the reference does Molini teach or suggest that a severity level is calculated for a group of events. As discussed above in the arguments presented for claims 1, 8, and 15, Molini only teaches assigning a criticality level to an individual message instead of a group of messages. Therefore, Molini does not teach calculating a severity level for a group of events. Similarly, nowhere in the above sections does Molini mention calculating a severity level for a group, let alone calculating a severity level for the group based on a number of event sets within each of the groups, the source attribute of the event sets within each of the groups, the target attribute of the event sets within each of the groups, and the event category attribute of the event sets within each of the groups. Molini is only concerned with filtering incoming messages one message at a time based on characteristics, such as a time of receipt. Molini is not concerned with calculating a severity level for the incoming messages as a group. Therefore, Molini does not and would not teach that the severity levels are calculated based on at least one of the number of event sets within each of the groups, the source attribute of the event sets within each of the groups, the target attribute of the event sets within each of the groups, and the event category attribute of the event sets within each of the groups, as recited in claims 2, 9, and 16 of the present invention.

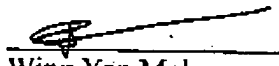
With regard to dependent claim 4, which is representative of dependent claims 11 and 18 with regard to similarly recited subject matter, instead of calculating the threshold value based on at least one of the source attribute of the event sets within the group, the target attribute of the event sets within the group, the event category attribute in each event set of the group, and the number of attributes in each event set of the group that are held constant across all of the event sets in the group, Molini fails to even mention calculating a threshold value.

The Examiner alleges that Molini teaches the feature of calculating the threshold value at column 7, lines 50-63 and column 8, lines 48-55, where Molini teaches that the threshold value is greater than or equal to 10 percent. The Examiner's allegation is erroneous. When read in combination with claims 1, 8, and 15, Molini fails to mention a threshold value that is calculated and compared to severity levels of the groups to report a group to the user if the severity level of a group exceeds the threshold value. As discussed above, Molini only teaches a criticality level of a single message instead of a severity level of a group of messages. In addition, contrary to a threshold value that is calculated and compared to severity levels of the groups to report a group to the user if the severity level of a group exceeds the threshold value, Molini merely teaches a minimum threshold of 10 percent or greater. Nowhere in the reference does Molini teach that the

threshold value is calculated and compared to severity levels of the groups. Therefore, Molini fails to teach the features of claims 4, 11, and 18 of the present invention.

With regard to dependent claim 7, which is representative of claims 14 and 21 with regard to similarly recited subject matter, instead of aggregating a subset of the groups into a combined group, Molini merely assesses a mapping of relationships from a database. The Examiner alleges that Molini teaches these features at column 9, lines 30-32, where Molini merely teaches a database that contains mapping of a combination of destination indicator and origin indicator associated with a corresponding zone, a destination indicator associated with a corresponding zone and an origin indicator associated with a corresponding zone. However, these mappings represent relationships between zone identifiers of attacks, source addresses of attacks, and destination addresses of attacks. The mappings do not represent a subset of groups of events that is aggregated into a combined group. Molini does not aggregate a subset of the relationships in the database into a combined group. Molini merely assess the relationships in the database to assign a detected attack to a specific zone indicator (column 9, lines 1-3). Therefore, Molini does not teach the features of claims 7, 14, and 21 of the present invention.

In view of the above, in addition to their dependency on independent claims 1, 8, and 15, Appellants respectfully submit that Molini also fails to teach the specific features of dependent claims 2-7, 9-14, and 16-21 of the present invention. Accordingly, Appellants respectfully request the withdrawal of rejection of claims 2-7, 9-14, and 16-21 under 35 U.S.C. § 102(e).



Wing Yan Mok
Reg. No. 56,237
**YEE & ASSOCIATES, P.C.**
PO Box 802333
Dallas, TX 75380
(972) 385-8777

## CLAIMS APPENDIX

The text of the claims involved in the appeal are:

1. A method in a data processing system for reporting security situations, comprising the steps of:

logging events by storing event attributes as an event set, wherein each event set includes a source attribute, a target attribute and an event category attribute;

classifying events as groups by aggregating events with at least one attribute within the event set as an identical value; and

calculating severity levels for the groups;

reporting a group from the groups to a user as a situation, if a severity level of the group exceeds a threshold value.

2. The method of claim 1, wherein the severity levels are calculated based on at least one of the number of event sets within each of the groups, the source attribute of the event sets within each of the groups, the target attribute of the event sets within each of the groups, and the event category attribute of the event sets within each of the groups.

3. The method of claim 1, wherein the events include at least one of a web server event, an electronic mail event, a Trojan horse, denial of service, a virus, a network event, an authentication failure, and an access violation.

4. The method of claim 1, further comprising:

calculating the threshold value based on at least one of the source attribute of the event sets within the group, the target attribute of the event sets within the group, the event category attribute in each event set of the group, and the number of attributes in each event set of the group that are held constant across all of the event sets in the group.

5. The method of claim 1, wherein the target attribute represents one of a computer and a collection of computers.

6. The method of claim 1, wherein the source attribute represents one of a computer and a collection of computers.

7. The method of claim 1, further comprising:

aggregating a subset of the groups into a combined group.

8. A computer program product in a computer readable medium for reporting security events, comprising instructions for:

logging events by storing event attributes as an event set, wherein each event set includes a source attribute, a target attribute and an event category attribute;

classifying events as groups by aggregating events with at least one attribute within the event set as an identical value; and

calculating severity levels for the groups;

reporting a group from the groups to a user as a situation, if a severity level of the group exceeds a threshold value.

9. The computer program product of claim 8, wherein the severity levels are calculated based on at least one of the number of event sets within each of the groups, the source attribute of the event sets within each of the groups, the target attribute of the event sets within each of the groups, and the event category attribute of the event sets within each of the groups.

10. The computer program product of claim 8, wherein the events include at least one of a web server event, an electronic mail event, a Trojan horse, denial of service, a virus, a network event, an authentication failure, and an access violation.

11. The computer program product of claim 8, comprising additional instructions for:

calculating the threshold value based on at least one of the source attribute of the event sets within the group, the target attribute of the event sets within the group, the event category attribute in each event set of the group, and the number of attributes in each event set of the group that are held constant across all of the event sets in the group.

12. The computer program product of claim 8, wherein the target attribute represents one of a computer and a collection of computers.

13. The computer program product of claim 8, wherein the source attribute represents one of a computer and a collection of computers.

14. The computer program product of claim 8, comprising additional instructions for:

aggregating a subset of the groups into a combined group.

15. A data processing system for reporting security events, comprising:

a bus system;

a memory;

a processing unit, wherein the processing unit includes at least one processor; and

a set of instructions within the memory,

wherein the processing unit executes the set of instructions to perform the acts of:

logging events by storing event attributes as an event set, wherein each event set includes a source attribute, a target attribute and an event category attribute;

classifying events as groups by aggregating events with at least one attribute within the event set as an identical value; and

calculating severity levels for the groups;

reporting a group from the groups to a user as a situation, if a severity level of the group exceeds a threshold value.

16. The data processing system of claim 15, wherein the severity levels are calculated based on at least one of the number of event sets within each of the groups, the source attribute of the event sets within each of the groups, the target attribute of the event sets within each of the groups, and the event category attribute of the event sets within each of the groups.

17. The data processing system of claim 15, wherein the events include at least one of a web server event, an electronic mail event, a Trojan horse, denial of service, a virus, a network event, an authentication failure, and an access violation.

18. The data processing system of claim 15, wherein the processing unit executes the set of instructions to perform the act of:

calculating the threshold value based on at least one of the source attribute of the event sets within the group, the target attribute of the event sets within the group, the event category attribute in each event set of the group, and the number of attributes in each event set of the group that are held constant across all of the event sets in the group.

19. The data processing system of claim 15, wherein the target attribute represents one of a computer and a collection of computers.

20. The data processing system of claim 15, wherein the source attribute represents one of a computer and a collection of computers.

21. The data processing system of claim 15, wherein the processing unit executes the set of instructions to perform the act of:

aggregating a subset of the groups into a combined group.

## EVIDENCE APPENDIX

There is no evidence to be presented.

## RELATED PROCEEDINGS APPENDIX

There are no related proceedings.